REMARKS

Claims 1-26, 28-33 and 35-40 are now pending in this application. The non-final Office Action mailed May 26, 2005, 2005 rejected claims 1-26, 28-33 and 35-40. Claims 1 and 28 have been amended in this response. Claim 1 is amended solely to correct an obvious grammatical error, and is not related to patentability. No new matter is added by these amendments. For the reasons discussed in detail below, Applicant submits that the pending claims are patentable over the art of record and respectfully request that the Examiner pass this application to issue.

Claim Rejections Under 35 U.S.C. §112:

The Office Action rejected claim 28 under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Specifically, the Office Action indicates that the word "decompressing" makes the claim indefinite and unclear, because the claim 28 and corresponding independent claim 26 do not specify that the content was compressed. Applicant respectfully disagrees, since the word "content" can be interpreted to include content in a compressed form. Nevertheless, without narrowing the scope of the invention, applicant has amended claim 28 to explicitly state that the decrypted content unit comprises a compressed content unit and that the method further comprises decompressing the compressed content unit. Support for the amendment is found at numerous locations in the specification, including pg. 9, lines 7-12. Accordingly, the rejection of claim 28 35 U.S.C. 112, second paragraph, should be withdrawn.

Claim Rejections Under 35 U.S.C. §103 over Al-Salqan & Ansell:

The Office Action rejected claims 1-4, 6-16, 18-22, 24-26, 28, 29, 31-33, 35-37, 39 and 40 under 35 U.S.C. §103(a) as being unpatentable over U.S. patent No. 6,160,891 to Al-Salqan (hereinafter "Al-Salqan") in view of U.S. Patent No. 6,610,891 to Ansell et al. (hereinafter "Ansell). Applicant respectfully traverses this rejection. To establish a prima facie case of obviousness, the cited references must disclose or suggest each limitation of a claim. The Office Action does not cite particular elements of each reference as disclosing or suggesting each limitation of applicant's independent claims. Nor does the Office Action indicate how elements of one reference relate to elements of another reference. Instead, the Office Action cites portions of Ansell as disclosing

some of the limitations missing from Al-Salqan, and cites the entire abstract, the entire specification, and four out of five figures shown in Al-Salqan as disclosing the remaining limitations of the independent claims. The Office Action further state "[a]lso see the entire [Ansell] reference for detail in relationship with Al-Salqan's reference)." (Office Action, pg 4, lines 13-14.) It is unclear to the applicant which elements of each reference supposedly disclose each limitation of applicant's claims and how the elements of each reference relate to each other to achieve the claimed invention. Thus, applicant first contends that the Office Action does not satisfy basic requirements of the Administrative Procedure Act, which requires all federal agencies, including the US Patent Office, to provide a substantial evidentiary basis for its findings, which a reasonable mind might accept as adequate to support its conclusion. (See e.g., In re Peterson, 315 F.3d 1325, 65 USPQ2d 1379 (Fed. Cir. 2003) and In re Thrift, 298 F.3d 1357, 63 USPQ2d 2002 (Fed. Cir. 2002).) Nevertheless, applicant attempts to analyze the references as discussed below.

Al-Salqan is directed to recovery of cryptographic keys. Al-Salqan defines a key, as "any other information that is concealed from the public and used in any manner to decrypt an encrypted message or used to obtain such a key." (Al-Salqan , col. 3, lines 55-62.) By definition, a key concealed from the public is a private key. Al-Salqan uses private information, or encoded private information, to encrypt a private key or a key password. (See Al-Salqan abstract, col. 4, lines 4-52, and col. 6, lines 61-67.) Al-Salqan explains that "[p]rivate information is information that would likely be known only by the principal of the key received at input 206 [i.e., the private key], such as social security number, mother's maiden name, and other similar information." (Al-Salqan, col. 4, lines 4-6.) The encrypted private key is then encrypted again into a key recovery file. In particular, the encrypted private key is "again encrypted, for example using asymmetric encryption, using the public key of a trusted party . . . The result may be stored as a key recovery file by the principal of the private key or another party." (Al-Salqan , abstract, and see col. 7, lines 1-7.) The key recovery file is stored for safe keeping in the event the private key is lost or otherwise unavailable such that messages could no longer be decrypted. (See Al-Salqan col. col. 2, lines 43-49, col. 5, lines 2-5, and col. 7, lines 7-10.)

The Office Action indicates that Al-Salqan discloses the limitations of the independent claims, including the following limitations of indendent claim 1:

(1) selectively encrypting at least a portion of the content stream using a content key;

(2) encrypting the content key using a screener key; and

(3) encrypting the screener key using a public key.

By comparison, it appears that the Office Action means to make the following equivalencies:

Al-Salqan Element	Claim Limitation
message	portion of the content stream
private key	content key
private information (or encoded private information)	screener key
public key of a trusted party	public key

The Office Action does not rely on Al-Salqan as disclosing the additional claim limitation that the public key is bound to a player such that the public key is unique to the player. Instead, the Office Action appears to indicate that Ansell discloses a public key of a player and that this public key is bound to the player. Specifically, the Office Action refers to "col. 2, lines 36-53 where the player has binding public and private key, and where player plays content stream; . . ." (Office Action, pg. 4, lines 9-11.) Ansell actually states:

> In particular, the keys are kept in a passport data structure which can represent either a machine binding or a user binding.
>
> In the machine binding, the passport contains a private key and a certificate that includes a public key which is the reciprocal of the private key. The private key is encrypted using a hardware identifier specific to the computer system to which the passport is bound. . . . The public key is used to encrypt a master key with which the content is encrypted and to create therefrom a media key which is included with the content along wit the certificate of the machine-bound passport. As a result, the private key is required to decrypt the media and to recover the master key and therefore to decrypt the content. (Ansell, col. 2, lines 33-49.)

Ansell further explains that "[m]edia key 302 is included with the encrypted content" (Ansell, col. 10, line 29.) However, the media key is not further encrypted. Ansell refers to media in the form of storage media "such as audio compact discs (CDs) and digital video discs (DVDs). Thus, the encrypted content is stored on a CD or DVD. Similarly, a media key is also stored on the CD or DVD. However, Ansell does not disclose or suggest that the media key is encrypted with the master key as the content is encrypted with the master key. On the contrary, the master key is encrypted with the public key to form the media key. Thus, assuming arguendo that the machines (computer systems) of Ansell can be equated to the claimed player, the following equivalencies are logical:

Ansell Element	Claim Limitation
content	portion of the content stream
master key	content key
public key (or encoded private information)	screener key
Media key is not encrypted	so no equivalent to claimed public key

By the above comparisons, it is clear that Ansell can not be combined with Al-Salqan to achieve the claim limitations. The public key of Ansell would have to be somehow related to the private information of Al-Salqan. However, by definition, private information can not be public, and a public key can not be private. Thus, Ansell and Al-Salqan teach away from each other.

In addition, Ansell discloses private information that is expressly used for user-binding, which is distinctly differentiated from machine-binding. For example, Ansell states that "the user-bound passport requires that the user provide more sensitive, private information." (Ansell, col. 3, lines 19-20.) Ansell explains "[f]or example, the user-passport can include credit card information of the user sufficient to charge funds to the credit card, e.g., credit card number, expiration, and cardholder name. During playback of content, the private user information is displayed. Therefore, sharing one's passport includes sharing one's credit." (Ansell, col. 3, lines 3-9.) This is "a disincentive to sharing one's [user-defined] password [] included in the user-bound passport" which deters people from sharing their password with others who could then access the encrypted content without paying for the right to access the content. (Ansell, col. 2, line 65 through col. 3, line 1.)

Ansell's expressed use of private information that is distinctly NOT bound to a machine or player, teaches away from any interpretation that Al-Salqan's private information can be associated with a public key that is bound to a machine or player.

There is also no disclosure of suggestion that Al-Salqan's private information can be equated to applicant's claimed screener key. As indicated above, Al-Salqan's private information is information that would likely be known only by the principal of the key received at input 206, such as social security number, mother's maiden name, and other similar information." (Al-Salqan, col. 4, lines 4-6.) In contrast, the claimed screener key is defined in terms of the specification as "generated using any of a variety of encryption/decryption symmetric key mechanisms" and "asymmetric key mechanisms may also be employed without departing from the scope or spirit of the present invention." (Spec., pg. 5, lines 1-8.) Since a screener key can be asymmetric (e.g., public), a screener key can not be equivalent to Al-Salqan's private information.

In addition, Applicants disagree that Al-Salqan's message is equivalent to a portion of a content stream as claimed, and disagree that one of ordinary skill in the art would be motivated to select and combine Al-Salqan with Ansell to include a content stream.

The reasons above can also be applied in reverse for decryption limitations in the independent claims. Thus, for at least the reasons discussed above, the rejection of independent claims 1, 8, 15, 26, and 32 under 35 U.S.C. §103(a) should be withdrawn. Dependent claims are patentable for at least the same reasons as the independent claims from which the dependent claims depend. Accordingly, the rejection of dependent claims 2-4, 6, 7, 9-14, 16, 18-22, 24, 25, 28, 29, 31, 33, 35-37, 39, and 40 under 35 U.S.C. §103(a) should also be withdrawn.

Claim Rejections Under 35 U.S.C. §103 over Al-Salqan, Ansell, & Downs:

The Office Action rejected claims 5, 17, 23, 30 and 38 under 35 U.S.C. §103(a) as being unpatentable over Al-Salqan in view of Ansell, and further in view of U.S. Patent No. 6,226,618 to Downs et al (hereinafter "Downs"). Applicant respectfully traverses this rejection. Downs is directed to securely providing data to a user by sending an encrypted key to a an intermediary clearing house, which decrypts the key and re-encrypts the key with a different public key, before

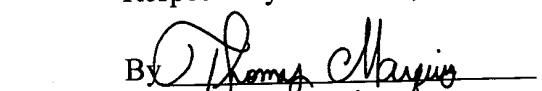
sending the re-encrypted key to the user. (See Downs abstract.) Downs does not disclose or suggest the limitations that are missing from Al-Salqan and Ansell. Thus, the rejected dependent claims 5, 17, 23, 30 and 38 are patentable for at least the same reasons discussed above with regard to corresponding independent claims 1, 15, 26, and 32. Accordingly, the rejection of dependent claims 5, 17, 23, 30 and 38 under 35 U.S.C. §103(a) should be withdrawn.

CONCLUSION

In view of the above amendment and remarks, applicant believes the pending application is in condition for allowance. Accordingly, the Examiner is respectfully requested to pass this application to issue. Should any further aspects of the application remain unresolved, the Examiner is invited to telephone applicant's attorney at the number listed below.

Dated: August 12, 2005

Respectfully submitted,

By 

Thomas R. Marquis
Registration No.: 46,900
DARBY & DARBY P.C.
P.O. Box 5257
New York, New York 10150-5257
(206) 262-8900
(212) 527-7701 (Fax)
Attorneys/Agents For Applicant

Customer No. 07278